

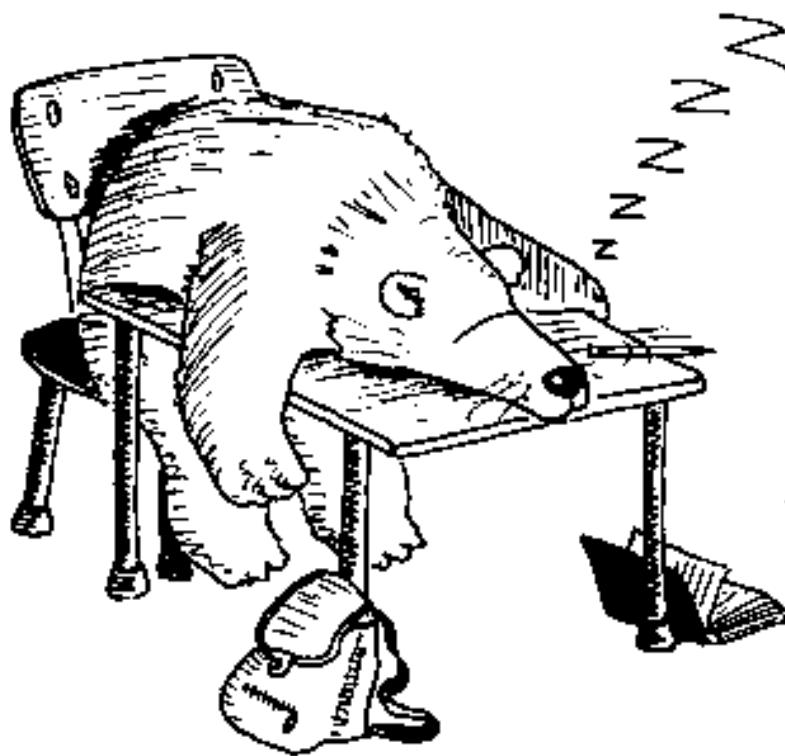
The background of the slide is a stylized, artistic representation of a particle accelerator. It features a central circular structure with concentric rings and radial lines, resembling a cross-section of a synchrotron or a similar high-energy physics facility. The colors are primarily dark blue, purple, and green, with some red and white highlights. The overall effect is a sense of depth and complexity, typical of scientific visualization.

Introduction to Safety Systems in Research Accelerators

Hazard Assessment and Risk
Analysis

USPAS

June, 2004



Eventually Randolph was forced to leave University due to his tendency to hibernate through lectures.

© Uwe Oehler, DrIguana@chembio.uoguelph.ca

Most encountered words from senior management?

“I do not want any surprises”



Hazard and risk analysis are a means to that end...

Hazard Analysis

- ❖ Hazard analysis uncovers and identifies hazards that exist in the workplace, generally focusing on a particular activity, project, or system.
- ❖ Basic information for risk based decisions
- ❖ Develop a means to:
 - ❖ Communicate
 - ❖ Track
 - ❖ Quantify
 - ❖ Allocate mitigation measures
 - ❖ Verify effectiveness
- ❖ Hazard analysis can also be referred to as *hazard recognition*, based upon the above definition.

Anticipate

Hazard assessment of a proposed facility or system should occur before design criteria or other, less formal work-description documents are drafted, ideally even before initial concepts are finalized.

Definitions

- ❖ Hazard – *a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event).*
- ❖ Hazard Level – *the combination of severity and likelihood of occurrence*

Definitions - continued

- ❖ Accident – *an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.*
- ❖ Mishap – *Department of Defense term for **accident** which is defined as an unwanted or uncontrolled release of energy or a toxic exposure.*
- ❖ Near miss/incident – *an event that involves no loss (or only minor loss) but with the potential for loss under different circumstances.*

Definitions - continued

- ❖ *Safety – freedom from accidents or losses*
- ❖ *Reliability – the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time under stipulated environmental conditions.*
- ❖ *Error – a design flaw or deviation from a desired or intended state.*

Definitions - continued

- ❖ Severity of occurrence – *the worst possible accident that could result from the hazard given the environment in its most unfavorable state.*
- ❖ Probability, or likelihood of occurrence – *may be specified either quantitatively or qualitatively.*
- ❖ Mishap probability – *is the probability that a mishap will occur during the planned life expectancy of the system. [MIL-STD-882D]*

Definitions - continued

- ❖ Risk – *is the hazard level combined with (1) the likelihood of the hazard leading to an accident (sometimes called danger) and (2) hazard exposure or duration (sometimes called latency).*
 - ❖ Correct way to combine all elements of risk is unknown
 - ❖ Parameter values of each function are also unknown
 - ❖ No agreement on how to combine probability, severity and non-probabilistic factors
 - ❖ Comparison of catastrophic but unlikely events with likely but less serious events is unknown
 - ❖ Must involve qualitative judgment and personal values

Definitions - continued

- ❖ Hazard Analysis – *the identification of hazards and the assessment of hazard level.*
- ❖ Risk Analysis – *includes hazard analysis plus the addition of identification and assessment of environmental conditions along with exposure or duration.*
 - ❖ Often used interchangeably with hazard analysis
 - ❖ Reliability often used incorrectly as a measure of risk

The Risk Components

RISK

Hazard Level

Hazard
severity

Likelihood of
hazard occurring

Hazard
exposure

Likelihood of
hazard leading
to an accident



Factors Affecting Risk Components

- ❖ Introduction of new hazards
- ❖ Lessons learned that are passed down through codes and standards of practice for known hazards
- ❖ New engineering specializations and technologies for which codes & standards have not been developed.
- ❖ Older, simpler technologies are replaced w/ newer, more complex technologies.

Factors Affecting Risk Components

- ❖ Redundancy may increase complexity
- ❖ Increasing complexity of hazards
- ❖ Exposure
- ❖ Energy
- ❖ Automation
- ❖ Centralization
- ❖ Scale
- ❖ Pace of technological change in the system

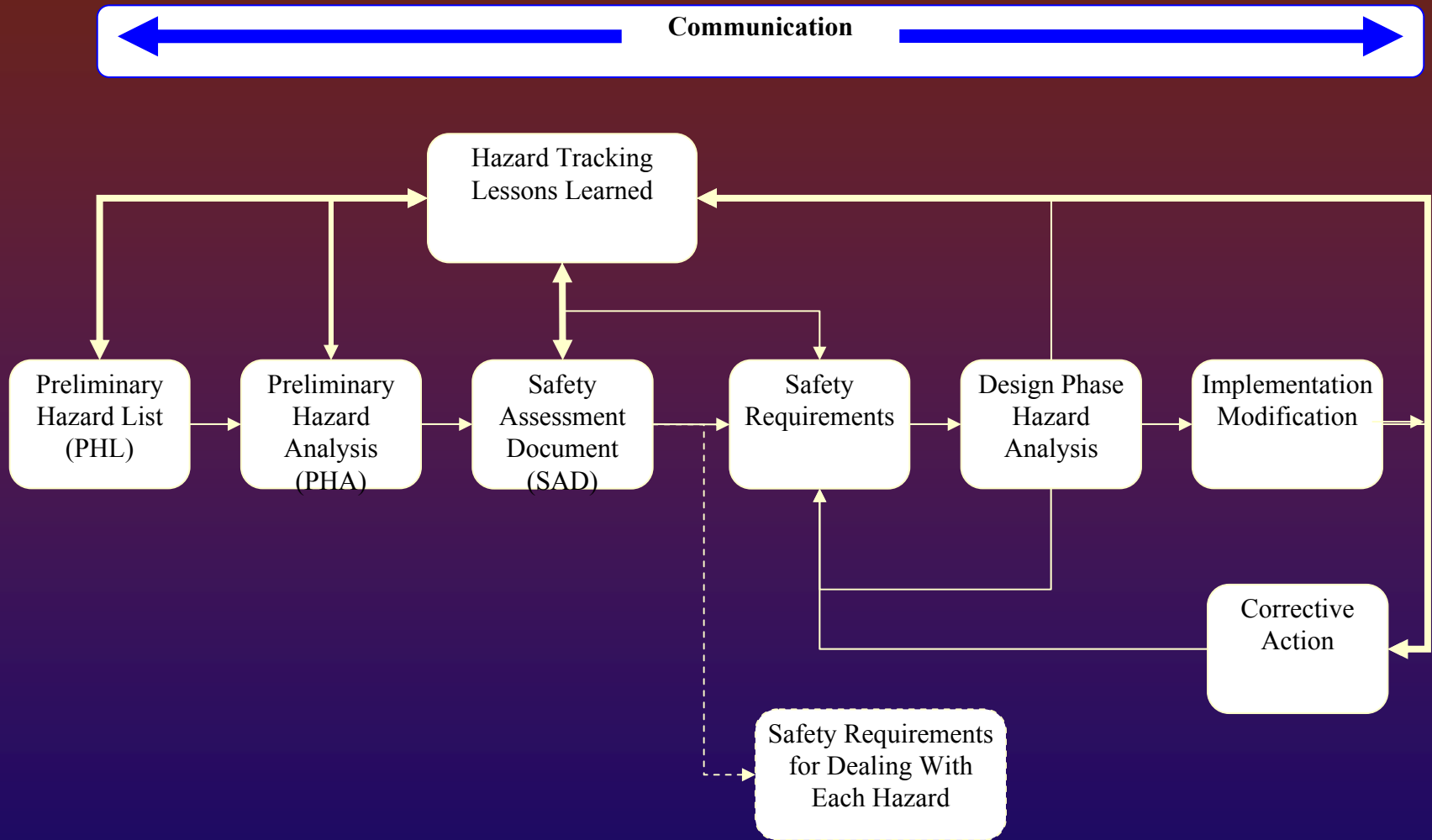
Hazard Assessment: Identification

- ❖ Identify hazards and the possible accidents that might result from each hazard.
 - ❖ Process should be systematic
 - ❖ Entail detailed analysis of system hardware and software
 - ❖ Evaluate environment in which it will exist
 - ❖ Include intended use or application

Hazard Identification Processes

- ❖ Preliminary Hazard Assessment (PHA)
- ❖ Preliminary Safety Assessment Review (PSAR)
- ❖ Preliminary Safety Assessment Document (PSAD)

Hazard Management Lifecycle



Hazard Identification Sources

- ❖ Sources of information
 - ❖ Historical hazard and mishap data
 - ❖ Accidents
 - ❖ Occurrence events
 - ❖ Lessons learned from other systems
 - ❖ Hazards that occur over the lifetime of the system
 - ❖ Mean time to failure of system components

PHL Form

Hazard And Risk Analysis
Revision A. June 2004

Page 1 of 3

Title:		ASIS PHL Example		Hazard Analysis Worksheet								To be completed during PHL		
Date:		PHL4/20/04 PHA FHA										To be completed during PHA		
Evaluator:		K. Mahoney										To be completed during Final HA		
Facility:		USPAS-A-TRON		Location: Univ. Wisc. Madison										
Purpose:		Preliminary Hazard Li								Risk Mitigation				
Reviewed/ Comments	Hazard Tracking Number	Hazard Description	Risk Analysis						Hazard Controls	Control Method	Control Risk Reduction			
			Hazard Type	Hazard Target	Exposure	Severity	Likelihood	Risk Code						
<input type="checkbox"/>	1-1	Prompt ionizing radiation in beam enclosure due to source other than beam.	Radiological	Employee										
<input type="checkbox"/>	2-1	Exposed energized electrical bus on dipole magnets in beam enclosure.	Electrical	Employee										
<input type="checkbox"/>	3-1	Oxygen deficient environment due to helium leak	ODH	Employee										
<input type="checkbox"/>	4-1	Microwave radiation in excess of 5mW/cm2 due to open waveguide.	Electromagnet	Employee										
<input type="checkbox"/>	5-1	Nitric Acid precipitated in beam dump from beam ionization.	Chemical	Employee										
<input type="checkbox"/>	5-2	Nitric Acid precipitated in beam dump from beam ionization.	Chemical	Equipment										

PHL Approved: _____

Date: _____

Hazard/Risk Assessment

- ❖ Having identified the hazards, one must assess the risks by considering the severity and likelihood of bad outcomes. If the risks are not sufficiently low, then additional controls or alternate methods must be applied.
- ❖ Risk increases if either likelihood or severity [*magnitude of loss*] increases provided the other component does not decrease proportionally.

Tailoring Your Risk Definition

- ❖ No task is completely without risk.
- ❖ Must develop tailored risk matrix, based upon acceptable risk, in order to identify what is considered *sufficiently low*
- ❖ Must define “*acceptable risk*”

Risk Class

❖ Example Risk Classification (IEC61508-5)

I Unacceptable

II Undesirable

III Action Recommended (ALARP)

IV Broadly Acceptable

❖ Classifications are developed inside the organization and approved by senior management



Acceptable Risk

- ❖ What is it?
 - ❖ The threshold level below which risk will be tolerated
- ❖ To whom is the risk posed?
 - ❖ Generally the risk is posed to those who are not defining it
- ❖ By whom is it judged acceptable?
 - ❖ Senior management based upon input from technical experts

Risk Assessment: Severity

- ❖ Evaluate the severity, or consequences, of each possible accident and rank order them by severity of the outcome.
 - ❖ Determine the potential negative impact of each hazard scenario on
 - ❖ Personnel
 - ❖ Equipment
 - ❖ Operations
 - ❖ Public
 - ❖ Environment
 - ❖ The system itself

Risk Assessment: Likelihood

- ❖ Likelihood, or Probability, assignment
 - ❖ Qualitative
 - ❖ Quantitative
- ❖ Estimate the probability of each possible accident.
 - ❖ Past history of accidents/incidents
 - ❖ Industry benchmarks

Likelihood/Probability Definition

- ❖ Can be defined in terms of occurrences per
 - ❖ Units of time
 - ❖ Events
 - ❖ Population
 - ❖ Items
 - ❖ Activity

Risk Assessment Tools

- ❖ To determine what actions to take to eliminate or control a hazard, a system of determining the level of risk is needed.
- ❖ Risk tool should enable you to properly understand the level of risk involved relative to what it will cost in schedule and mitigation \$\$

Risk Tool Development

- ❖ In early design stages, severity consideration is all that's needed since you should first try to eliminate the hazards by design
- ❖ When all hazards cannot be eliminated, probability factors become important
- ❖ General risk assessment tools are available however it's best if you use tools tailored to your individual program

Simple Probability Functions

$$P(\text{Event})=P(\text{Hazard})*P(\text{Severity})*P(\text{Likelihood})*P(\text{Exposure})$$

The Risk/Hazard Matrix (RHM)

- ❖ Allows you to assign a risk value to each hazard scenario
- ❖ Can rank order hazard scenarios
- ❖ Identify potential mitigation alternatives
- ❖ Evaluate alternatives in terms of risk reduction (use your matrix)
- ❖ Prioritize mitigation tasks

Risk Matrix

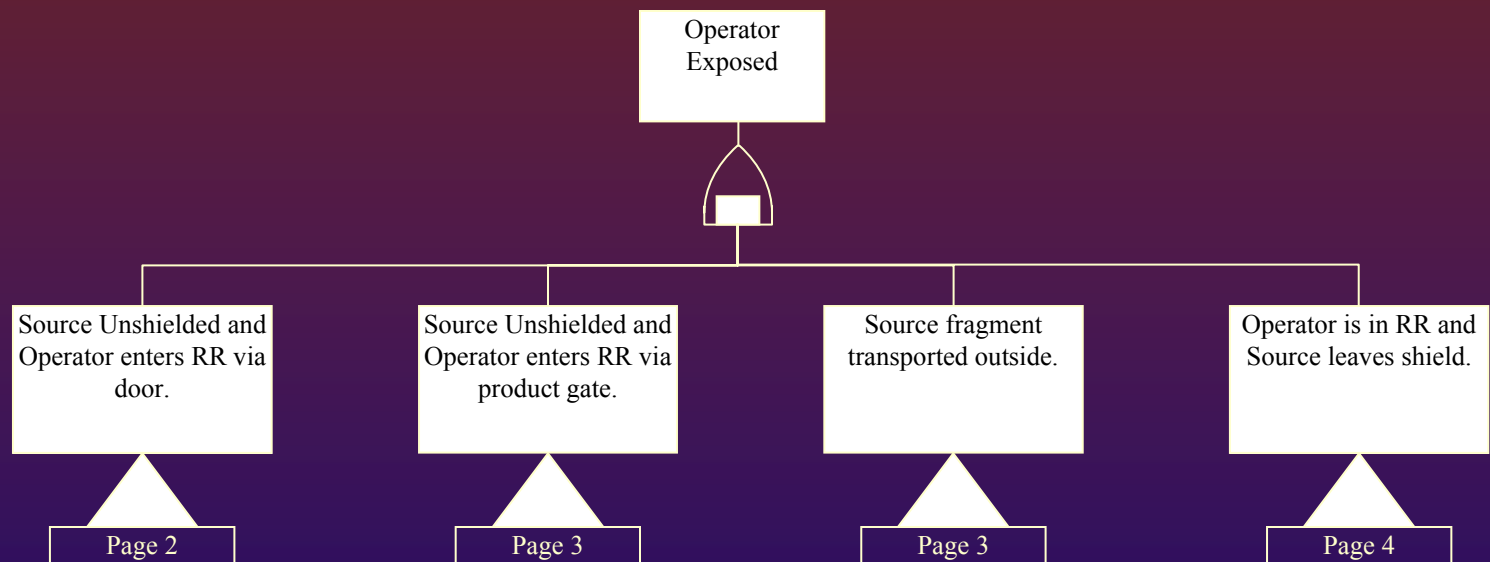
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV
Frequency	Catastrophic	Critical	Marginal	Negligible
	Consequence			

	A	B	C	D	E	F	G	
1	Today's Date	6/29/2004						
2								
3	Project	USPAS						
4	Evaluator	K. Mahoney						
5	Date	6/22/2004						
6	Hazard	Shock from Energized Magnets						
7	Constraint 1	50-250VDC						
8	Constraint 2	<5mA						
9								
10	Likelihood							
11	Consequence							
12								
13								User Defined Ra
14	Risk Matrix		Color code	Intolerable		0	4	
15				Undesirable		4	5	
16				Tolerable		5	7	
17				Acceptable		7	>	
18	User Defined Likelihood							
19	Immanent	0 Frequent		3	2	1	0	
20	1day-1year	1 Probable		4	3	2	1	
21	1-10 years	2 Occasional		5	4	3	2	
22	Over life of facility	3 Remote		6	5	4	3	
23	100-1000 years	4 Unlikely		7	6	5	4	
24	>1000 years	5 Impossible		8	7	6	5	
25				3	2	1	0	
26		Consequences		Minimal	Marginal	Critical	Catastrophic	
27				First Aid	< 5 Lost Work Days	> 5 lost work days	Death or Disability	

Fault Tree Analysis (FTA)

- ❖ Widely used in aerospace, electronics and nuclear industries
- ❖ Primarily a means for analyzing causes of hazards, not identifying hazards
- ❖ Top-down search method, with the top event having been foreseen
- ❖ Four basic steps: (1) system definition; (2) fault tree construction; (3) qualitative analysis; and (4) quantitative analysis

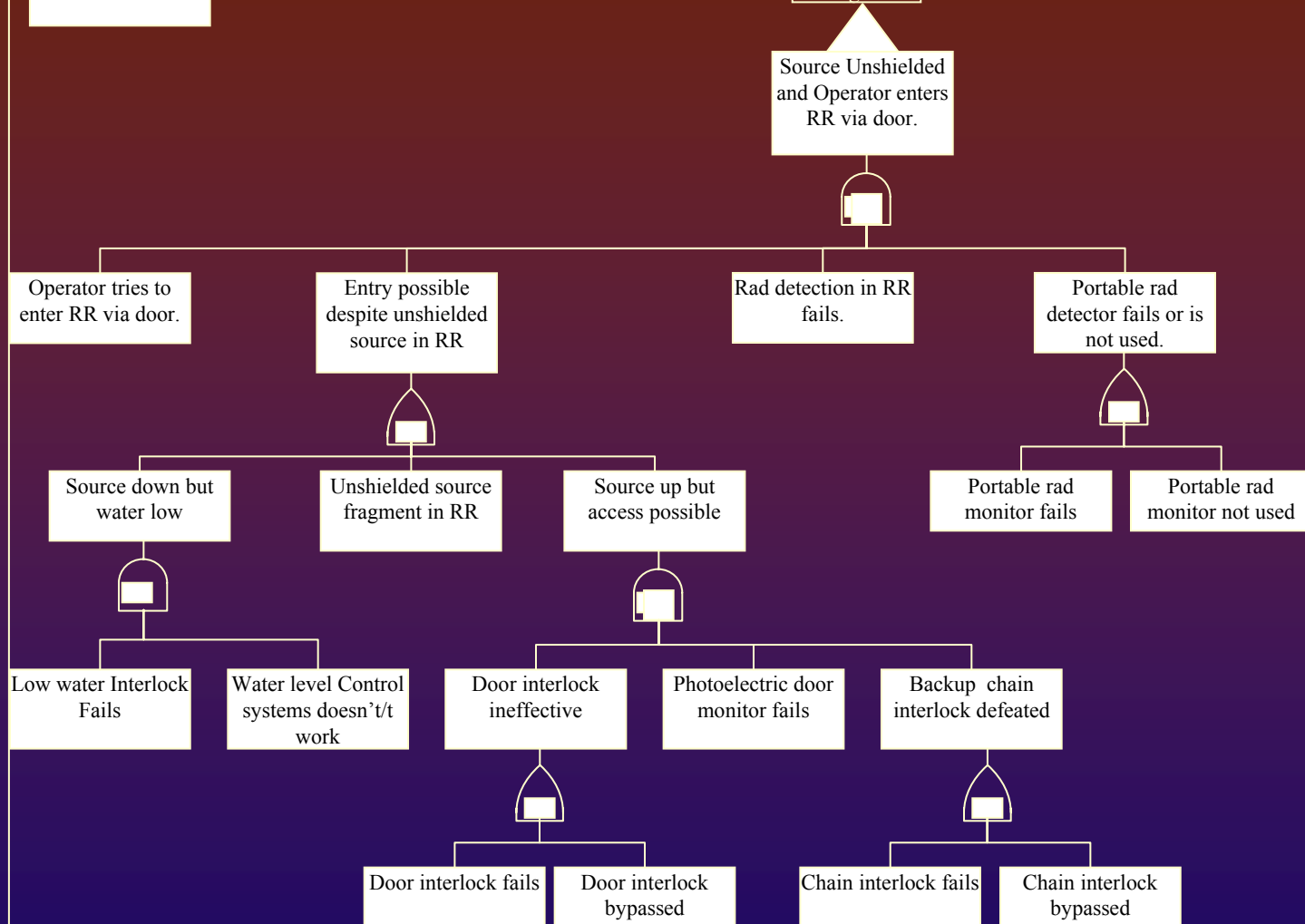
Qualitative Fault Tree



Qualitative Fault Tree

PAGE 2

Page 1

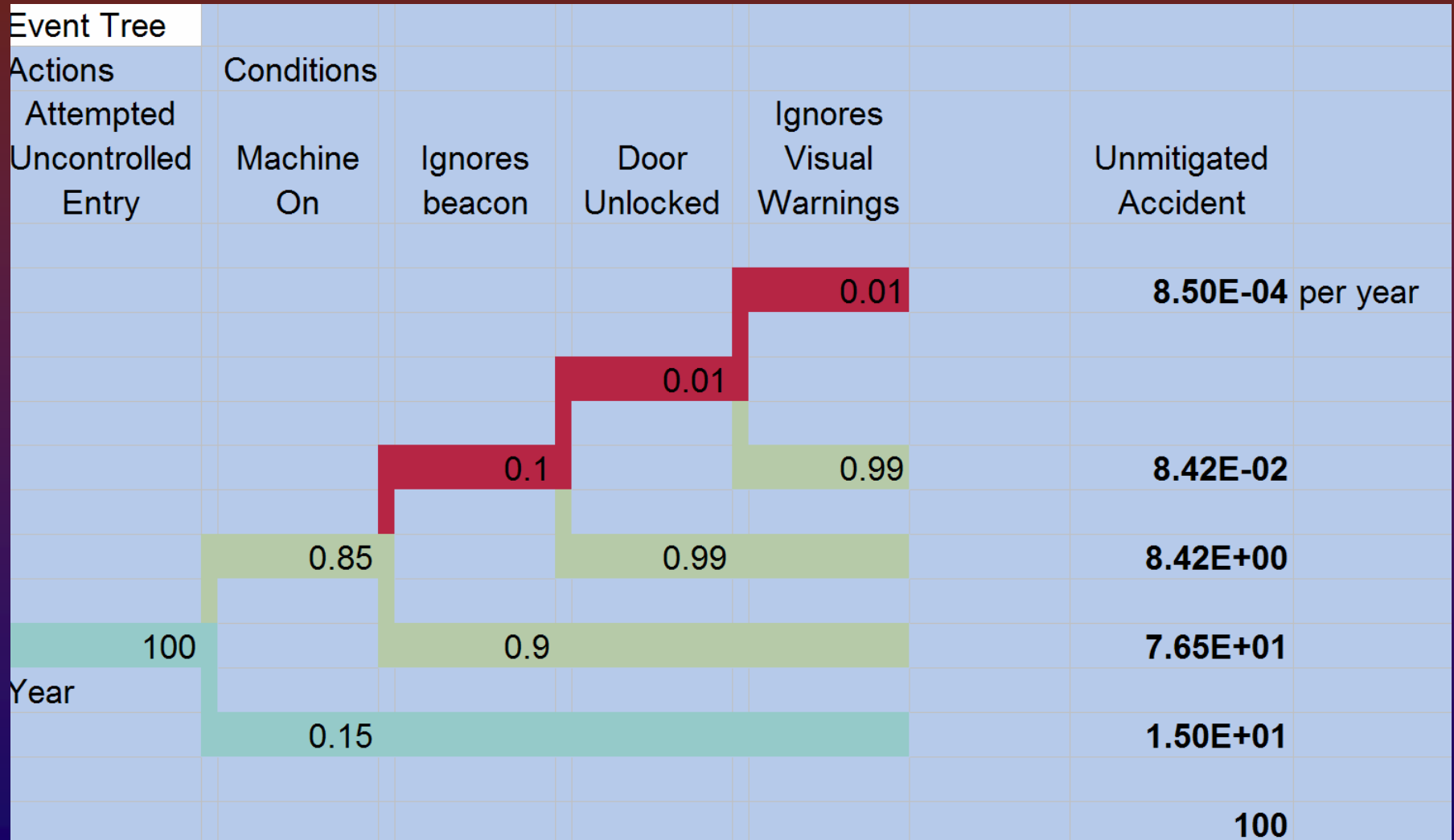


From ICRP Publication 76 pp34

Event Tree Analysis (ETA)

- ❖ An adaptation of general decision tree whereby a problem is broken up into smaller parts to which the FTA is then applied.
- ❖ Uses forward search to identify possible outcomes of an event
- ❖ Principally used in nuclear power plants
- ❖ Drawn from left to right
- ❖ Based upon a binary state system [success or failure]
- ❖ Tend to be quite large

Example Event Tree



Failure Modes & Effects Analysis (FMEA)

- ❖ Form of reliability analysis
- ❖ Emphasizes successful functioning rather than hazards & risk
- ❖ Uses forward search based upon chain-of-events model
- ❖ All significant failure modes must be known in advance
- ❖ Doesn't consider effects of multiple failures (except for subsequent effects it might produce)

Failure Modes & Effects Analysis (FMEA)

- ❖ Analyzes single failure modes
 - ❖ Determines effects on all other system components and on overall system
 - ❖ Probabilities and seriousness of each failure mode's results are calculated
 - ❖ Critical effects are added to get failure probability for entire system
- ❖ Failures rates predicted from generic rates developed from experience over time

Failure Modes & Effects Analysis (FMEA) - Uses

- ❖ Identify redundancy and fail-safe design requirements
- ❖ Single-point failure modes
- ❖ Inspection points
- ❖ Spare parts requirements
- ❖ Strength of technique is completeness but it is also time consuming

Hazard & Operability Analysis (HAZOP)

- ❖ Primarily used by the chemical industry
- ❖ Focuses on safety & efficient operations
- ❖ Assumes accidents are caused by deviations from design or operating intent
- ❖ Systematic, qualitative technique
- ❖ Able to identify “unreviewed” safety issues
- ❖ It is labor-intensive

Layer of Protection Analysis (LOPA)

- ❖ Used to more realistically assign risk reduction factors to non-safety system functions
 - ❖ Operator Response
 - ❖ Dedicated Control System safety functions

Hazards Control Precedence

- ❖ The accepted precedence for dealing with hazards is:
 - Eliminate the hazard (the most effective method but oftentimes incompatible with the mission objective)
 - Reduce the hazard in a manner that prevents or minimizes conditions that could lead to unacceptable risk

Hazard Elimination

- ❖ Eliminate hazards through design selection
 - ❖ Process change
 - ❖ Material substitution
- ❖ Reduce hazards by using
 - ❖ safety features or devices
 - ❖ detection and warning systems
 - ❖ procedures and training (may involve use of personal protective equipment)

Classes of Hazard Controls

- ❖ Engineering - methods of controlling employee exposures by modifying the source or inherent design of the process or work configuration
- ❖ Administrative – Procedural controls which depend upon employee awareness and compliance for their effectiveness
- ❖ Personal Protective Equipment (least preferred)

Two Types of Controls

- ❖ Active Controls - require some action to prevent or mitigate the hazard.
 - ❖ Safety interlock system
 - ❖ Access control system
- ❖ Passive Controls - relies on basic physical principles to prevent/minimize a hazard's effects
 - ❖ Shielding
 - ❖ Labyrinths
 - ❖ Barriers – locked doors & enclosed fencing
 - ❖ Distance

Hazard Controls Verification

- ❖ Verify effectiveness of controls through
 - ✓ Analysis – design reviews, computer modeling
 - ✓ Testing – commissioning activities, system certification/functional testing, readiness reviews
 - ✓ Inspection
- ❖ Look for new hazards during testing that may have been overlooked

Residual Risk

- ❖ The risk that remains after all planned risk management measures have been implemented:
 - ❖ Must be documented along with reasons why it exists
 - ❖ Must be reviewed and accepted by management
 - ❖ Management review must be documented
 - ❖ Generally managed by administrative controls

Documentation

- ❖ Records of hazard reviews should be incorporated into the overall project design documentation.
 - ❖ It preserves your methods and rationale so that you are able to undertake a comparable review more efficiently in the future.
 - ❖ It provides a defensible basis for your system during a permitting or agency review.
 - ❖ It augments the customary discipline found in good engineering and architectural design practices.

Tracking Systems

- ❖ System performance over its life cycle
 - ❖ System failures and corrective actions
 - ❖ Maintenance and certification tests
 - ❖ Inspection findings
 - ❖ Change control
 - ❖ Modifications
 - ❖ Upgrades
 - ❖ System “add-ons”

Communicate!

- ❖ Managers
- ❖ System managers
- ❖ System integrators
- ❖ System support staff
- ❖ System operators
- ❖ EH&S staff
- ❖ Affected workers